(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **11086435 A**

(43) Date of publication of application: **30 . 03 . 99**

(51) Int. Cl **G11B 20/10**
G09C 1/00
G09C 1/00
G09C 5/00
H04L 9/32
H04N 1/387
H04N 5/91
H04N 7/08
H04N 7/081

(21) Application number: **10190825**

(22) Date of filing: **06 . 07 . 98**

(30) Priority: **07 . 07 . 97 JP 09181459**

(71) Applicant: **MATSUSHITA ELECTRIC IND CO LTD**

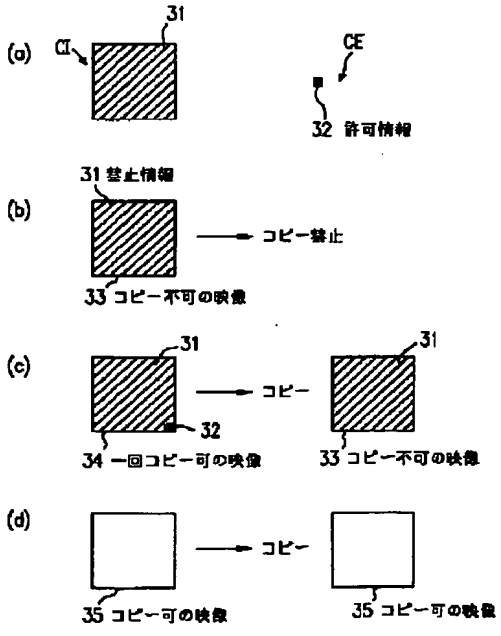
(72) Inventor: **IBARAKI SUSUMU**
KATSUTA NOBORU

(54) **DATA CONTROL METHOD, DATA CONTROL INFORMATION EMBEDDING METHOD, DATA CONTROL INFORMATION DETECTION, DATA CONTROL INFORMATION EMBEDDING DEVICE, DATA CONTROL INFORMATION DETECTOR AND RECORDER**

(57) Abstract:

PROBLEM TO BE SOLVED: To control copying propriety and the number of copying times and to protect a copyright by embedding prohibition information into data, such as videos and voices.

SOLUTION: The prohibition information 31 is embedded into the videos and permission information 32 is embedded therein by using digital signature, etc., if N times of copying is okay. At the time of reproduction of the data, the presence or absence of the permission information 32 is investigated and a permission flag is set at a 1 or 0. If the permission flag is 1, the permission information 32 is deleted and the copying of the data is made possible. If the permission flag is 0, the prohibition information 31 is detected. A prohibition flag is then made 1 or 0. If the prohibition flag is 1, a copying okay or denial flag is set at the 0 and the copying of the data is prohibited.



(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平11－86435

(43)公開日　平成11年(1999)３月30日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｇ１１Ｂ　20/10		Ｇ１１Ｂ　20/10	Ｆ
Ｇ０９Ｃ　1/00	６４０	Ｇ０９Ｃ　1/00	６４０Ｂ
	６６０		６６０Ｄ
5/00		5/00	
Ｈ０４Ｌ　9/32		Ｈ０４Ｎ　1/387	

審査請求　有　請求項の数18　ＯＬ　（全 16 頁）　最終頁に続く

(21)出願番号　特願平10－190825

(22)出願日　平成10年(1998)７月６日

(31)優先権主張番号　特願平9－181459

(32)優先日　平９(1997)７月７日

(33)優先権主張国　日本（ＪＰ）

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地

(72)発明者　茨木　晋
大阪府門真市大字門真1006番地　松下電器産業株式会社内

(72)発明者　勝田　昇
大阪府門真市大字門真1006番地　松下電器産業株式会社内

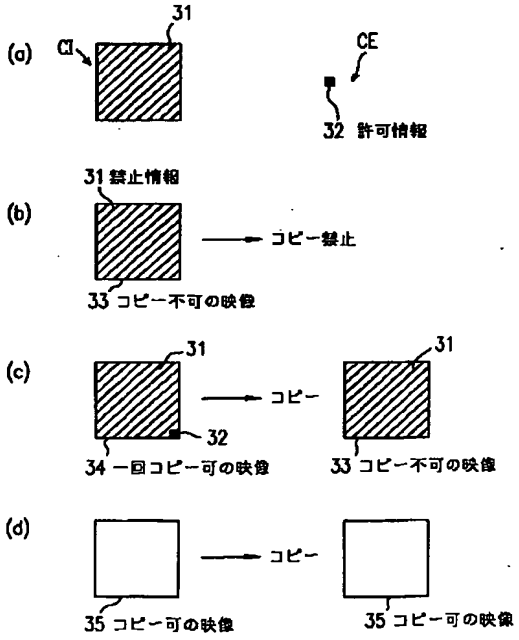
(74)代理人　弁理士　山本　秀策

(54)【発明の名称】　データ制御方法、データ制御情報埋込方法、データ制御情報検出方法、データ制御情報埋込装置、データ制御情報検出装置及び記録装置

(57)【要約】

【課題】映像や音声などのデータにコピー禁止情報を埋め込むことにより、コピー可否やコピー回数の制御を行い、著作権を保護すること。

【解決手段】禁止情報３１を映像に埋め込み、Ｎ回コピー可ならデジタル署名等を用いて許可情報３２を埋め込む。データの再生時には、許可情報３２の有無を調べ、許可フラグを１又は０に設定する。許可フラグが１であれば、許可情報３２を削除し、データのコピーを可能にする。許可フラグが０であれば、禁止情報３１を検出する。そして禁止フラグを１又は０にする。禁止フラグが１であれば、コピー可否フラグを０にし、データのコピーを禁止する。



1

【特許請求の範囲】

【請求項１】　データのコピーを禁止する場合は禁止情報を前記データ中に埋め込み、

前記データのコピーをＮ（Ｎは自然数）回許可する場合は前記禁止情報を前記データ中に埋め込むと共に、Ｎ個の許可情報を前記データ中に埋め込み、

前記データのコピーに先立ち、前記データから前記許可情報が検出された場合には、前記データの少なくとも１つの前記許可情報を無効にして前記データのコピーを許可し、

前記データのコピーに先立ち、前記データから前記許可情報が検出されず、前記禁止情報が検出された場合には、前記データのコピーを禁止することを特徴とするデータ制御方法。

【請求項２】　前記許可情報は、デジタル署名ｆ（Ｍ）であって、

前記デジタル署名ｆ（Ｍ）は、前記データからデジタルコードＭを抽出し、該デジタルコードＭに基づいて求められることを特徴とする請求項１記載のデータ制御方法。

【請求項３】　データのコピーを禁止する場合は禁止情報を前記データ中に埋め込み、

前記データのコピーをＮ（Ｎは自然数）回許可する場合は前記禁止情報を前記データ中に埋め込むと共に、Ｎ個の許可情報を前記データ中に埋め込むことを特徴とするデータ制御情報埋込方法。

【請求項４】　前記許可情報は、

前記データから一意に得られるデジタルコードＭに対するデジタル署名ｆ（Ｍ）であることを特徴とする請求項３記載のデータ制御情報埋込方法。

【請求項５】　データのコピーに先立ち、前記データから予め定めれた許可情報が検出された場合には、前記許可情報を無効にして前記データのコピーを許可し、

前記データのコピーに先立ち、前記データから前記許可情報が検出されず、予め定められた禁止情報が検出された場合には、前記データのコピーを禁止することを特徴とするデータ制御情報検出方法。

【請求項６】　データのコピーに先立ち、前記データ中のデジタル署名ｆ（Ｍ）を認証できた場合には、前記データのコピーを許可し、

前記データのコピーに先立ち、前記データ中のデジタル署名ｆ（Ｍ）を認証できない場合には、前記データのコピーを禁止し、

前記署名ｆ（Ｍ）は、前記データから得られるデジタルコードＭに基づいて認証されることを特徴とするデータ制御情報検出方法。

【請求項７】　データの少なくともコピーの禁止を示す禁止情報を前記データ中に埋め込む禁止情報埋込手段と、

前記データのコピーをＮ（Ｎは自然数）回許可したいとき、前記禁止情報埋込手段による禁止情報の埋め込みに伴い、Ｎ個の許可情報を前記データ中に埋め込む許可情報埋込手段と、を具備することを特徴とするデータ制御情報埋込装置。

2

【請求項８】　前記許可情報埋め込み手段は、

前記データからデジタルコードＭを抽出するコード抽出手段を有することを特徴とする請求項７記載のデータ制御情報埋込装置。

【請求項９】　前記許可情報埋込手段は、前記コード抽出手段で抽出された前記デジタルコードＭ、及び前記データの作成者が保持する第１の暗号鍵に基づいてデジタル署名ｆ（Ｍ）を生成する署名手段と、

前記署名手段で生成されたデジタル署名ｆ（Ｍ）を前記許可情報として前記データ中に埋め込む署名埋込手段と、を有することを特徴とする請求項８記載のデータ制御情報埋込装置。

【請求項１０】　データに埋め込まれた禁止情報及び許可情報を抽出するデータ制御情報検出装置であって、

前記データから前記許可情報を検出する許可情報検出手段と、

前記データの前記許可情報を無効にする許可情報無効手段と、

前記データから前記禁止情報を検出する禁止情報検出手段と、

前記許可情報検出手段によって前記許可情報が検出された場合には、コピー可否フラッグを可にして出力し、前記許可情報検出手段によって前記許可情報が検出されずに、前記禁止情報検出手段によって前記禁止情報が検出された場合には、前記コピー可否フラッグを不可にして出力する判定手段と、を具備することを特徴とするデータ制御情報検出装置。

【請求項１１】　前記許可情報検出手段は、

前記データからデジタルコードＭを抽出するコード抽出手段を有することを特徴とする請求項１０記載のデータ制御情報検出装置。

【請求項１２】　前記許可情報検出手段は、

前記データに埋め込まれたデジタル署名ｆ（Ｍ）を抜き出す署名抜出手段と、

前記コード抽出手段によって抽出された前記デジタルコードＭと第２の暗号鍵に基づいてデジタル署名ｆ（Ｍ）を生成し、この生成されたデジタル署名ｆ（Ｍ）と前記署名抜出手段によって抜き出された前記デジタル署名ｆ（Ｍ）を対比し、これによって前記デジタル署名ｆ（Ｍ）が認証された場合にコピー許可フラグを有効にして出力する認証手段と、を具備することを特徴とする請求項１１記載のデータ制御情報検出装置。

【請求項１３】　データを記録媒体に記録する記録装置であって、

前記データから前記許可情報を検出する許可情報検出手段と、

前記データの前記許可情報を無効にする許可情報無効手段と、
前記データから前記禁止情報を検出する禁止情報検出手段と、
前記許可情報検出手段によって前記許可情報が検出された場合には、コピー可否フラッグを可にして出力し、前記許可情報検出手段によって前記許可情報が検出されずに、前記禁止情報検出手段によって前記禁止情報が検出された場合には、前記コピー可否フラッグを不可にして出力する判定手段と、
前記判定手段によって前記コピー可否フラグ許可とされた場合はデータの記録を行い、前記コピー可否フラグが不可とされた場合は記録を行わないデータ記録手段と、を具備することを特徴とする記録装置。

【請求項１４】　データの処理を禁止する場合は禁止情報を前記データ中に埋め込み、
前記データの処理をＮ（Ｎは自然数）回許可する場合は前記禁止情報を前記データ中に埋め込むと共に、Ｎ個の許可情報を前記データ中に埋め込み、
前記データの処理に先立ち、前記データから前記許可情報が検出された場合には、前記データの少なくとも１つの前記許可情報を無効にして前記データの処理を許可し、
前記データの処理に先立ち、前記データから前記許可情報が検出されず、前記禁止情報が検出された場合には、前記データの処理を禁止することを特徴とするデータ制御方法。

【請求項１５】　データの処理を禁止する場合は禁止情報を前記データ中に埋め込み、
前記データの処理をＮ（Ｎは自然数）回許可する場合は前記禁止情報を前記データ中に埋め込むと共に、Ｎ個の許可情報を前記データ中に埋め込むことを特徴とするデータ制御情報埋込方法。

【請求項１６】　データの処理に先立ち、前記データから予め定めれた許可情報が検出された場合には、前記許可情報を無効にして前記データの処理を許可し、
前記データの処理に先立ち、前記データから前記許可情報が検出されず、予め定められた禁止情報が検出された場合には、前記データの処理を禁止することを特徴とするデータ制御情報検出方法。

【請求項１７】　データの処理の禁止を示す禁止情報を前記データ中に埋め込む禁止情報埋込手段と、
前記データの処理をＮ（Ｎは自然数）回許可したいとき、前記禁止情報埋込手段による禁止情報の埋め込みに伴い、Ｎ個の許可情報を前記データ中に埋め込む許可情報埋込手段と、を具備することを特徴とするデータ制御情報埋込装置。

【請求項１８】　データに埋め込まれた禁止情報及び許可情報を抽出するデータ制御情報検出装置であって、
前記データからＮ（Ｎは自然数）個の許可情報が検出されたときには、前記データの少なくとも１つの前記許可情報を無効にし、許可フラグを有効にして出力する許可情報検出・削除手段と、
前記データから禁止情報が検出されたときには、禁止フラグを有効にして出力する禁止情報検出手段と、
前記許可フラグが有効か、又は前記禁止フラグが有効でないときに、可否フラグを可にして出力し、前記許可フラグが有効でなく、かつ前記禁止情報が有効であるときに、前記可否フラグを不可にして出力する判定手段と、
を具備することを特徴とするデータ制御情報検出装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、音声ソフトや映像ソフトなどに代表される著作権の保護の対象となるデータを、複製（コピー）又はデータ処理（編集）することを防止するため、記録データの複製の許可又は不許可の制御を行うコピー制御情報を付加するデータ制御情報埋め込み方法及びその装置と、その情報を抽出するデータ制御情報検出方法及びその装置と、データ制御情報埋め込み方法及びデータ制御情報検出方法を併せたデータ制御方法とに関するものである。

【０００２】

【従来の技術】映像にコピー制御情報を埋め込む方法として、またコピー制御情報の検出方法として、パッチワークと呼ばれる方法がある。この方法は、日経エレクトロニクスの1997年２月24日号（ＮＯ．683）の149ｐ～162ｐの「電子透かしを支えるデータハイディング技術（上）」（及びW. Bender , D. Gruhl, N. Morimoto, A. Lu. “Techniques for data hiding”, IBM Systems Journal, Vol 35, NOS 3&4, 1996）に紹介されている。以下、従来技術におけるコピー制御情報埋め込み方法と、その情報を抽出するコピー制御情報検出方法について説明する。

【０００３】従来のコピー制御情報埋込方法として、１枚の映像にコピー可否ビット（１ビット）を埋め込む手順を説明する。コピー可否ビットとして、コピーが可のときは１、コピーが不可のときは０とする。擬似乱数により映像から２点（Ａｉ、Ｂｉ）を選ぶ。次に、埋め込むビットが１のときは、Ａｉの輝度レベルＹａｉをｄだけ上げ、Ｂｉの輝度レベルＹｂｉをｄだけ下げる。逆に、埋め込むビットが０の時は、Ａｉの輝度レベルをｄだけ下げ、Ｂｉの輝度レベルをｄだけ上げる。このときｄの値は１～５の間の整数である。これらの処理をｎ回（ｎは通常１万程度）繰り返す。

【０００４】次に従来のコピー制御情報検出方法を説明する。まず、擬似乱数により映像から情報埋込時と同じ位置の２点の輝度レベル（画素情報）、即ち（Ｙａｉ＋ｄ、Ｙｂｉ－ｄ）又は（Ｙａｉ－ｄ、Ｙｂｉ＋ｄ）を抽出する。そしてこれら２点の差を計算する。これらの処理を夫々の位置についてｎ回繰り返し、これらの差の平

均を求める。この平均がｄ以上であれば、埋め込まれているビットが１であるとし、－ｄ以下であれば埋め込まれているビットが０であるとする。平均が－ｄ以上、ｄ以下のとき、情報が埋め込まれていないとする。

【０００５】ここでは、Ｙａｉ－Ｙｂｉの期待値を０と推定している。また（Ｙａｉ＋ｄ）－（Ｙｂｉ－ｄ）の期待値は２ｄ、（Ｙａｉ－ｄ）－（Ｙｂｉ＋ｄ）の期待値は－２ｄである。これにより、平均値０からのずれの閾値を、ｄ及び－ｄとして判定を行っている。更に正確な判定を行うためには、差の統計分布を求め、分散の推定値からのずれによっても、検出可能である。

【０００６】以上の様に、従来のコピー制御情報埋込方法及びコピー制御情報検出方法によれば、１ビットのコピー可否フラグの埋め込みと検出が可能である。更なる方法として、選択した画素に一様にレベルｄを加算や減算を行うのではなく、映像の特徴に応じて画素ごとに埋め込むレベルを変化させつつ、それらのレベルを各画素の輝度に減算あるいは加算し、これらの平均がレベルｄとなるようにして情報を埋め込めば、埋め込んだ後の映像の劣化を抑え、不正行為を更に困難にすることができる。

【０００７】

【発明が解決しようとする課題】しかるに、コピー制御情報埋込方法および検出方法においては、コピーの許可、禁止を示すだけではなく、コピーをＮ回だけ許可するようなコピー回数を制御することが要求されている。コピー回数を制御するには、コピー時にコピー制御情報の書き換えが必要である。例えば、１回コピー可能なソフトには、１回コピー可能であることを示すコピー制御情報を埋め込む。そしてコピー時にこれをコピー禁止であることを示すコピー制御情報に書き換えなければならない。

【０００８】このようなコピー制御情報の書き換えを、従来のコピー制御情報埋込方法及びびコピー制御情報検出方法で実現するためには、コピー制御情報埋込方法とコピー制御情報検出方法の両方をユーザのコピー時に実行しなければならない。従来のコピー制御情報埋込方法は、コピー制御情報検出方法に比べて処理が困難であるので、ユーザが実現するのはコストアップにつながる。また、コピー制御情報埋込方法をユーザに公開することになるので、不正行為が容易に実行される恐れがある。

【０００９】本発明は、このような従来の問題点に鑑みてなされたものであって、コピーの許可や禁止だけでなく、コピー回数の制御が可能で、不正処理が困難なデータ制御情報埋め込み方法及びその装置と、データ制御情報検出方法及びその装置を実現することを目的とする。またデータの編集や表示等のデータ処理を制限するデータ制御情報埋め込み方法及びその装置と、データ制御情報検出方法及びその装置を実現することも目的とする。

【００１０】

【課題を解決するための手段】このような課題を解決するため、本発明のデータ制御方法は、データのコピーを禁止する場合は禁止情報を前記データ中に埋め込み、前記データのコピーをＮ（Ｎは自然数）回許可する場合は前記禁止情報を前記データ中に埋め込むと共に、Ｎ個の許可情報を前記データ中に埋め込み、前記データのコピーに先立ち、前記データから前記許可情報が検出された場合には、前記データの少なくとも１つの前記許可情報を無効にして前記データのコピーを許可し、前記データのコピーに先立ち、前記データから前記許可情報が検出されず、前記禁止情報が検出された場合には、前記データのコピーを禁止している。

【００１１】１実施形態では、前記許可情報は、デジタル署名ｆ（Ｍ）であって、前記デジタル署名ｆ（Ｍ）は、前記データからデジタルコードＭを抽出し、該デジタルコードＭに基づいて求められる。

【００１２】本発明のデータ制御情報埋込方法は、データのコピーを禁止する場合は禁止情報を前記データ中に埋め込み、前記データのコピーをＮ（Ｎは自然数）回許可する場合は前記禁止情報を前記データ中に埋め込むと共に、Ｎ個の許可情報を前記データ中に埋め込んでいる。

【００１３】１実施形態では、前記許可情報は、前記データから一意に得られるデジタルコードＭに対するデジタル署名ｆ（Ｍ）である本発明のデータ制御情報検出方法は、データのコピーに先立ち、前記データから予め定めれた許可情報が検出された場合には、前記許可情報を無効にして前記データのコピーを許可し、前記データのコピーに先立ち、前記データから前記許可情報が検出されず、予め定められた禁止情報が検出された場合には、前記データのコピーを禁止している。

【００１４】１実施形態では、データのコピーに先立ち、前記データ中のデジタル署名ｆ（Ｍ）を認証できた場合には、前記データのコピーを許可し、前記データのコピーに先立ち、前記データ中のデジタル署名ｆ（Ｍ）を認証できない場合には、前記データのコピーを禁止し、前記署名ｆ（Ｍ）は、前記データから得られるデジタルコードＭに基づいて認証される。

【００１５】本発明のデータ制御情報埋込装置は、データの少なくともコピーの禁止を示す禁止情報を前記データ中に埋め込む禁止情報埋込手段と、前記データのコピーをＮ（Ｎは自然数）回許可したいとき、前記禁止情報埋込手段による禁止情報の埋め込みに伴い、Ｎ個の許可情報を前記データ中に埋め込む許可情報埋込手段とを具備している。

【００１６】１実施形態では、前記許可情報埋め込み手段は、前記データからデジタルコードＭを抽出するコード抽出手段を有する。

【００１７】１実施形態では、前記許可情報埋込手段は、前記コード抽出手段で抽出された前記デジタルコー

ドM、及び前記データの作成者が保持する第１の暗号鍵に基づいてデジタル署名ｆ（M）を生成する署名手段と、前記署名手段で生成されたデジタル署名ｆ（M）を前記許可情報として前記データ中に埋め込む署名埋込手段とを有する。

【００１８】本発明のデータ制御情報検出装置は、データに埋め込まれた禁止情報及び許可情報を抽出するデータ制御情報検出装置であって、前記データから前記許可情報を検出する許可情報検出手段と、前記データの前記許可情報を無効にする許可情報無効手段と、前記データから前記禁止情報を検出する禁止情報検出手段と、前記許可情報検出手段によって前記許可情報が検出された場合には、コピー可否フラッグを可にして出力し、前記許可情報検出手段によって前記許可情報が検出されずに、前記禁止情報検出手段によって前記禁止情報が検出された場合には、前記コピー可否フラッグを不可にして出力する判定手段とを具備している。

【００１９】１実施形態では、前記許可情報検出手段は、前記データからデジタルコードMを抽出するコード抽出手段を有する。

【００２０】１実施形態では、前記許可情報検出手段は、前記データに埋め込まれたデジタル署名ｆ（M）を抜き出す署名抜出手段と、前記コード抽出手段によって抽出された前記デジタルコードMと第２の暗号鍵に基づいてデジタル署名ｆ（M）を生成し、この生成されたデジタル署名ｆ（M）と前記署名抜出手段によって抜き出された前記デジタル署名ｆ（M）を対比し、これによって前記デジタル署名ｆ（M）が認証された場合にコピー許可フラグを有効にして出力する認証手段とを具備している。

【００２１】本発明の記録装置は、データを記録媒体に記録する記録装置であって、前記データから前記許可情報を検出する許可情報検出手段と、前記データの前記許可情報を無効にする許可情報無効手段と、前記データから前記禁止情報を検出する禁止情報検出手段と、前記許可情報検出手段によって前記許可情報が検出された場合には、コピー可否フラッグを可にして出力し、前記許可情報検出手段によって前記許可情報が検出されずに、前記禁止情報検出手段によって前記禁止情報が検出された場合には、前記コピー可否フラッグを不可にして出力する判定手段と、前記判定手段によって前記コピー可否フラグ許可とされた場合はデータの記録を行い、前記コピー可否フラグが不可とされた場合は記録を行わないデータ記録手段とを具備している。

【００２２】本発明のデータ制御方法は、データの処理を禁止する場合は禁止情報を前記データ中に埋め込み、前記データの処理をN（Nは自然数）回許可する場合は前記禁止情報を前記データ中に埋め込むと共に、N個の許可情報を前記データ中に埋め込み、前記データの処理に先立ち、前記データから前記許可情報が検出された場合には、前記データの少なくとも１つの前記許可情報を無効にして前記データの処理を許可し、前記データの処理に先立ち、前記データから前記許可情報が検出されず、前記禁止情報が検出された場合には、前記データの処理を禁止している。

【００２３】本発明のデータ制御情報埋込方法は、データの処理を禁止する場合は禁止情報を前記データ中に埋め込み、前記データの処理をN（Nは自然数）回許可する場合は前記禁止情報を前記データ中に埋め込むと共に、N個の許可情報を前記データ中に埋め込んでいる。

【００２４】本発明のデータ制御情報検出方法は、データの処理に先立ち、前記データから予め定めれた許可情報が検出された場合には、前記許可情報を無効にして前記データの処理を許可し、前記データの処理に先立ち、前記データから前記許可情報が検出されず、予め定められた禁止情報が検出された場合には、前記データの処理を禁止している。

【００２５】本発明のデータ制御情報埋込装置は、データの処理の禁止を示す禁止情報を前記データ中に埋め込む禁止情報埋込手段と、前記データの処理をN（Nは自然数）回許可したいとき、前記禁止情報埋込手段による禁止情報の埋め込みに伴い、N個の許可情報を前記データ中に埋め込む許可情報埋込手段とを具備している。

【００２６】本発明のデータ制御情報検出装置は、データに埋め込まれた禁止情報及び許可情報を抽出するデータ制御情報検出装置であって、前記データからN（Nは自然数）個の許可情報が検出されたときには、前記データの少なくとも１つの前記許可情報を無効にし、許可フラグを有効にして出力する許可情報検出・削除手段と、前記データから禁止情報が検出されたときには、禁止フラグを有効にして出力する禁止情報検出手段と、前記許可フラグが有効か、又は前記禁止フラグが有効でないときに、可否フラグを可にして出力し、前記許可フラグが有効でなく、かつ前記禁止情報が有効であるときに、前記可否フラグを不可にして出力する判定手段とを具備している。

【００２７】

【発明の実施の形態】以下、本発明の実施の形態について、添付図面を参照して説明する。

【００２８】（実施の形態１）本実施の形態１におけるデータ制御方法について説明する。図１は本実施の形態１のデータ制御方法の概要を示す説明図である。本実施の形態１で言うデータ制御とは、コピー制御を意味する。図１（ａ）に示す様に、信号ＣＩは画面全体に分散された信号であり、コピーの禁止情報３１を示す。信号ＣＥは画面の特定箇所に挿入された信号であり、１回のコピーの許可情報３２を示す。N回のコピーを許可する場合は、許可情報３２をN個画面に挿入する。

【００２９】信号ＣＩは、例えば画面全体に分散され、視認することはできないものである。これに対して、信

号ＣＥは、例えば画面の所定の角に挿入され、視認されなくても、視認されてもよい。

【００３０】図１（ｂ）はコピー不可の映像３３を示す。図１（ｃ）は１回コピー可の映像３４を示し、画面右下に許可情報３２が１つ挿入されている。図１（ｄ）はコピー可の映像３５を示し、画面全体に禁止情報３１が画面に挿入されていない。

【００３１】本実施の形態１が目的とするコピー制御とは、コピーフリーと、Ｎ回（以下の説明ではＮ＝１）コピー可と、コピー不可の３つの状態により映像信号の出力制御を行うものである。コピーフリー（コピー可）のときは、無条件でコピーを許可する。１回コピー可のときは、１回だけコピーを許可する。コピー不可のときは、映像の表示は許可してもコピーを一切禁止する。

【００３２】コピー不可の映像３３には、図１（ｂ）のように禁止情報３１を埋め込む。このコピー不可の映像３３が記録装置に入力されたとき、許可情報３２は検出されず、禁止情報３１が検出される。この場合は映像３３のコピーを禁止する。１回コピー可の映像３４に対しては、図１（ｃ）のように禁止情報３１と許可情報３２の両方を埋め込む。この映像３４をコピーするときには、許可情報３２が検出されるので、コピーを許可する。記録装置では、伝送路から該記録装置に転送されて来た映像３４の許可情報３２自身を削除して、映像３４のコピーを開始する。ここで、許可情報３２の削除においては、許可情報３２を全て削除しても良いし、許可情報３２の一部を削除しても良く、許可情報３２として検出不可能な状態、つまり許可情報を無効にすることが目的である。例えば、許可情報３２が８ビットの意味のある情報を持っていた場合、そのうちの1ビットを削除するだけでも良いし、８ビット全てを削除しても良い。あるいは、許可情報３２が２つの情報の組み合わせにより構成されていた場合には、そのうちの片方を削除しても良い。

【００３３】コピーした後の映像は許可情報３２だけが取り除かれているので、禁止情報３１が残り、コピー不可の映像３３となる。

【００３４】ただし、許可情報が２つ以上のＮ個埋め込まれていたＮ回コピー可の映像については、許可情報が１個削除されるので、（Ｎ－１）回コピー可の映像になる。

【００３５】コピーフリーの映像３５には、禁止情報３１も許可情報３２も埋め込まない。このコピーフリーの映像３５をコピーするときには、許可情報３２も禁止情報３１も検出されないので、無条件にコピーが許可される。

【００３６】以上のようなコピー制御方法によれば、コピーの禁止と許可の制御だけでなく、Ｎ回だけコピーを許可するような制御を実現できる。さらに、コピーするときに禁止情報の埋込方法や禁止情報の削除方法を公開する必要はない。このため、不正者が禁止情報を削除することが困難となる。また、コピー時に許可情報を埋め込まないので、その埋込方法は公開する必要はない。このため、不正者は許可情報を埋め込むことはできない。図１を用いた説明において、禁止情報を画面全体に埋め込むとしたが、これに限られるものではなく、画面の特定箇所に埋め込んでも良い。又図１を用いた説明において、許可情報を特定箇所に埋め込むとしたが、Ｎ＝１に限定される場合には、これに限られず、画面全体に埋め込んでも良い。

【００３７】次に、本実施の形態１のデータ制御方法を実現するための基本技術であるデータ制御情報埋込方法と、データ制御情報検出方法について、図２乃至図５を用いて説明する。

【００３８】図２は本実施の形態１のデータ制御情報埋込方法を示すフローチャートである。図４は本実施の形態１のデータ制御情報検出方法を示すフローチャートである。

【００３９】まず、図２で示すデータ制御情報埋込方法において、初期状態として、映像を（１）コピー不可、（２）１回コピー可、（３）コピーフリーの内、いずれの状態かを示す変数Ｓｔａｔｕｓを設定する。まずステップＳ１では、Ｓｔａｔｕｓがコピーフリーかどうかを判定し、コピーフリーの場合には処理を終了し、コピーフリーでない場合には、ステップＳ２に分岐する。ステップＳ２では、禁止情報３１を映像中に埋め込む。

【００４０】この埋め込み処理は、例えば従来技術のコピー制御情報の埋込方法など、映像中に１ビット以上の情報を埋め込むための任意の埋込方法で良い。特に、埋込方法がその検出方法よりも複雑である方法であればなお良く、その制限の元であれば、埋め込み方法によって本発明の効果が損なわれることはない。。このような映像に情報を埋め込む方法は、電子透かし（Ｗａｔｅｒ Ｍａｒｋ）と呼ばれ、従来技術で示した方法以外にも数多くの方法が知られている。例えば、日経エレクトロニクスの１９９７年２月２４日号（電子透かしがマルチメディア時代を守る）に紹介されている方法などがある。次のステップＳ３に進むと、Ｓｔａｔｕｓが１回コピー可か否かを判定し、１回コピー可でない場合に処理を終了し、１回コピー可の場合にはステップＳ４に分岐する。

【００４１】ステップＳ４では、許可情報３２を映像中に埋め込む。このステップＳ４は、例えば図３のフローチャートに示す様な処理であり、このフローチャートを参照して、このステップＳ４の許可情報の埋め込み処理を詳細に説明する。

【００４２】まず、ステップＳ２１では、情報を埋め込む映像の画素からその映像と一意に対応するコードＭを抜き出す。コードＭの抜き出し処理は、例えば映像中からｋ個の所定の各画素を選び、これらの画素のデータの

11

ＭＳＢ（最上位ビット）をｋビットのコードＭとする方法で実現できる。しかしこれに限定されず、映像から８×８画素のブロックをｋ個選び、これらのブロックの輝度値をｋビットのコードＭとする方法、映像の周波数成分を計算してその低周波成分を用いる方法など、映像からデジタルデータを一意に抜き出せる方法であれば、任意の方法で良い。

【００４３】次のステップＳ２２では、コードＭを用いてデジタル署名ｆ（Ｍ）を作成する。ここでデジタル署名について詳細に説明しておく。ユーザＡが映像の送信者、ユーザＢが映像の受信者とし、ユーザＡからユーザＢに映像のコードＭを署名Ｃ＝ｆ（Ｍ）に変換して送信する場合を考える。このとき、ユーザＡは署名Ｃを作成して映像を送信し、ユーザＢはその署名を認証、即ちその署名が正しいか否かを検証する。

【００４４】本実施の形態１に要求されるデジタル署名とは、次の性能が満たされればなんでも良い。

【００４５】（１）ユーザＢは署名Ｃを容易に認証できること。

【００４６】（２）ユーザＡは署名Ｃの作成は容易だが、ユーザＡ以外の者は署名Ｃの作成は困難であること。

【００４７】このデジタル署名の具体的な方法として、公開鍵暗号を利用する方法がある。ユーザＡは、署名を行う関数として署名関数Ｄ（第１の暗号鍵）を用意し、認証を行う関数として認証関数Ｅ（第２の暗号鍵）を用意する。ここで認証関数Ｅは署名関数Ｄの逆関数になるよう設定する。ユーザＡは署名関数Ｄを用いて、コードＭから署名Ｃを、Ｃ＝Ｄ（Ｍ）により作成する。ユーザＢは認証関数Ｅを用いて、Ｅ（Ｃ）がＭと一致するか否かを検証する。即ち認証関数Ｅは署名関数Ｄの逆関数なので、Ｃが正しい署名であれば、Ｅ（Ｃ）＝Ｅ（Ｄ（Ｍ））＝Ｍとなり、Ｃが正しい署名でなければ、Ｅ（Ｃ）とＭとは一致しない。

【００４８】ここで公開鍵暗号では、公開された認証関数Ｅから、秘密である署名関数Ｄを求めるのが困難であるという仕組みを、数学的な手法を用いて実現している。この実現例としては、ＲＳＡ暗号、Ｅｌｇａｍａｌ暗号等を利用したものがある。ＲＳＡ暗号では、署名関数Ｄを次の（１）式で定義する。

$$D(M)=M^{d} \bmod n \quad \cdots (1)$$

【００４９】また認証関数Ｅは次の（２）式で定義する。

$$E(C)=C^{e} \bmod n \quad \cdots (2)$$

【００５０】ここでｍｏｄｎは、ｎによる剰余演算、即ちｎで割った余りの整数を意味する（１），（２）式におけるｎ，ｅ，ｄは、ＥがＤの逆関数になるよう選択される。即ち次の（３）式が成立するよう選択される。

$$E(C)=C^{e} \bmod n=(M^{d})^{e} \bmod n$$
$$=M^{de} \bmod n=M \cdots (3)$$

12

ユーザＡは、大きな素数ｐ，ｑを用意し、ｎ＝ｐ×ｑとする。次に（ｐ－１）×（ｑ－１）＝φ（ｎ）なるオイラーの関数φ（ｎ）を定義する。次に関数φ（ｎ）と互いに素となる整数ｅを適当に設定する。即ち、φ（ｎ）とｅは、その最大公約数が１になる。そして次の（４）式が成立するようにｄを決定する。

$$e \times d \bmod \phi(n)=1 \quad \cdots (4)$$

このように決定されたｅ，ｄを用いれば、前述した（３）式が成立する。

【００５１】ユーザＡはｎとｅとを公開し、ｄ，ｐ，ｑを秘密にする。従って認証関数Ｅは公開されるが、署名関数Ｄは秘密にされる。ｐとｑを知っているユーザＡは、（４）式を用いてｅからｄを求めることができる。しかしｐとｑを知らないユーザＢは、ｎとｅからｄを求めることが困難となる。

【００５２】理解を容易にするため、ごく簡単な数値例を示す。例えば素数としてｐ＝５、ｑ＝１１を選ぶと、ｎ＝５５、φ（ｎ）＝４０となる。次にｅ＝７を選ぶと、（４）式から、７×２３ｍｏｄ４０＝１となり、ｄ＝２３が得られる。ユーザＡは、ｎ＝５５とｅ＝７を公開し、ｐ＝５、ｑ＝１１、ｄ＝２３を秘密にする。

【００５３】例えばＭ＝４２に対する署名は、次の（５）式のように計算される。

$$D(M)=42^{23} \bmod 55=3 \quad \cdots (5)$$

【００５４】これよりＣ＝３となる。ユーザＢは公開されている認証関数を用いて、次の（６）式の計算を行う。

$$E(C)=3^{7} \bmod 55=42 \quad \cdots (6)$$

【００５５】この結果、Ｅ（Ｃ）は当初のＭ＝４２と一致するので、正しい署名であることが認証される。

【００５６】ここでは、簡単のために、ｎを構成する素数ｐ，ｑとして小さい値を選んだが、暗号の安全性を高めるために、実際のｎは５１２ビット程度の大きさが用いられる。ｐ，ｑの値が２５６ビット幅としても、その大きさは１０進数に換算して、７７～７８桁程度の巨大な値になる。

【００５７】以上の説明は、公開鍵暗号を用いたデジタル署名であるが、これ以外にも、ナップザック問題に基づくデジタル署名や、ゼロ知識会話型証明を適用したデジタル署名などがあり、参考文献である辻井、笠原著「暗号と情報セキュリティ」（昭昇堂発行）に記載されている。

【００５８】さて、図２及び図３のフローチャートについて引き続き説明する。図３のステップＳ２２で、コードＭを用いてデジタル署名ｆ（Ｍ）を作成した後、ステップＳ２３で映像中に署名ｆ（Ｍ）を埋め込む。映像中への署名ｆ（Ｍ）の埋め込みの方法として、０は白、１は黒というような可視的なパターンで映像の端に埋め込む方法がある。しかしこの方法に限定せず、映像中から選択した画素のＬＳＢ（最下位ビット）を署名ｆ（Ｍ）

で置き換える方法、映像のブランキング区間に埋め込む方法、容易に削除可能な電子透かしを用いる方法など、複数ビットのコードを埋め込める方法であれば、任意の方法で良い。

【００５９】この様な許可情報の埋め込みの処理は、映像から一意に導き出せるコードＭを元にしたデジタル署名を許可情報として用いているので、秘密鍵ｄがなければ第３者が同じ署名を作成することは困難であり、新たに許可情報の埋め込みはできない。

【００６０】本実施の形態１のコピー制御情報埋込方法により、コピーフリーの場合には、映像には何も埋め込まず、１回コピー可の場合には禁止情報と１つの許可情報を映像に埋め込む。、そしてコピー不可の場合には禁止情報のみを映像に埋め込む。

【００６１】次に、図４を参照して、像からコピー制御情報を検出するための本実施の形態１のデータ制御情報検出方法について説明する。

【００６２】まず、ステップＳ５では、映像から許可情報３２の検出を行う。このステップＳ５は、例えば図５のフローチャートに示す様な処理であり、このフローチャートを参照して、このステップＳ５の許可情報の検出処理を詳細に説明する。

【００６３】図５のステップＳ２４において、映像に埋め込まれた署名ｆ（Ｍ）を検出する。次のステップＳ２５では、映像からコードＭを抜き出す。このコードＭの抜き出しは、図３のステップＳ２１でコードＭを抜き出したのと同じ処理でできる。

【００６４】次のステップＳ２６では、デジタル署名の認証を行う。このデジタル署名の認証は、ステップＳ２２で作成した署名の認証である。例えば、ＲＳＡ暗号の認証の場合、公開情報ｎと公開鍵ｅを用いる。署名ｆ（Ｍ）をＣとすると、署名の認証のための関数は前述した（２）式で表される。この結果が、（３）式で示すようにＭとなれば、認証可であり、Ｍと一致しなければ認証不可である。

【００６５】認証可であれば、許可情報が埋め込まれているので、ステップＳ２７に進み、許可フラグに１を代入する。ステップＳ２６で認証不可であれば、許可情報が埋め込まれていないので、ステップＳ２８に進み、許可フラグに０を代入する。本実施の形態１では上記のように許可フラグを生成したが、許可情報が埋め込まれている状態と、埋め込まれていない状態とを識別できる信号であれば、何でも良い。

【００６６】この様に図４のステップＳ５で許可情報を検出した後、ステップＳ６に進み、許可フラグを判定する。許可フラグが１の場合にはステップＳ７に分岐し、０の場合にはステップＳ８に分岐する。ステップＳ７では許可情報の削除を行う。この許可情報の削除は、ステップＳ４で埋め込まれた許可情報を、映像から取り除く処理であり、先程示したように、許可情報の少なくとも一部を削除する。ステップＳ７の処理後、ステップＳ１１に進み、コピー可否フラグを１にする。

【００６７】ステップＳ８では、禁止情報を検出する。これはステップＳ２で埋め込まれた禁止情報を検出することである。ここでは禁止情報がある場合には禁止フラグを１にし、ない場合には禁止フラグを０にする。その後ステップＳ９に進み、禁止フラグの判定を行う。禁止フラグが１の場合にはステップＳ１０へ分岐し、禁止フラグが０の場合にはステップＳ１１へ分岐する。禁止フラグの生成方法は、上記の方法に限らず、禁止情報が埋め込まれている状態と、埋め込まれていない状態を識別できる信号であれば、何でも良い。

【００６８】ステップＳ１０ではコピー可否フラグを０にし、ステップＳ１１ではコピー可否フラグを１に設定する。ここで、コピー可否フラグは、０がコピー禁止、１がコピー許可を示す信号である。なお、コピー可否フラグは、コピーの禁止と許可を識別できる信号であれば、任意の形態で良い。

【００６９】本実施の形態１のデータ制御情報検出方法により、許可情報が埋め込まれた映像は、許可情報が削除された後でコピーが許可される。許可情報も禁止情報も埋め込まれていない映像は、コピーが許可される。許可情報が埋め込まれておらず、禁止情報が埋め込まれている映像は、コピーが禁止される。

【００７０】以上説明したように、本実施の形態１では、１回コピー可からコピー不可への状態の変化を、許可情報の埋め込みと削除で実現している。さらにこの許可情報の埋め込みはデジタル署名に基づいており、削除や検出は容易であるが、秘密鍵ｄを知らない者にとっては、許可情報の埋め込みは困難である。このため不正にコピー許可に変更（書換え）することは困難である。さらに、禁止情報は許可情報と別の方法で埋め込んでおり、ユーザＢにはその検出方法のみを公開又は提供すれば良いので、ユーザＡは、その埋め込みや削除の方法を秘密にできる。

【００７１】また、本実施の形態１によれば、コピーの禁止と許可だけでなく、一回だけコピーを許可するような制御を実現できる。このため、従来と比べて不正が困難なデータ制御方法、あるいはデータ制御情報埋込方法及びデータ制御情報検出方法を実現できる。

【００７２】また、本実施の形態１では、１回コピー可を実現する方法について述べたが、コピー制御情報を埋め込む時に許可情報をＮ（Ｎは２以上の整数）回埋め込み、検出するときには許可情報が何個検出されても１個だけ削除することにより、Ｎ回コピー可という制御も実現可能である。

【００７３】なお、以上の説明では、コピーの禁止、１回許可、Ｎ回許可というデータ制御方法について説明したが、これに限られるものではなく、映像の再生の禁止、１回許可、Ｎ回許可という制御、更には映像の編集

又は加工といったデータ処理や、映像の表示も同様に制御することができる。

【００７４】また、映像信号を処理の対象としているが、音声信号や文書を処理の対象としてもよく、同様の効果が得られる。

【００７５】更に、許可信号として映像から一意に得られるコードMを元にしたデジタル署名を用いているが、これに限られるわけではなく、任意の埋め込み方法を用いることができる。即ち、ユーザＢに埋め込み方法を公開せず、削除と検出の方法のみを公開すれば良い。削除や検出の方法から、埋め込みの方法が類推できない方法や、削除や検出と比べて埋め込み処理の計算量が多いか、又は回路規模が複雑であるような方法であれば、更に不正に対して強くすることができる。この時、映像から一意に得られるコードMを元にして許可情報を作成することにより、映像と許可情報を１対１に対応させることができ、許可情報の不正な作成を困難にする。

【００７６】許可情報の埋め込み方法の他の例としては、許可情報が第１の許可情報と第２の許可情報の２つから構成され、第1の許可情報を第１の埋め込み方法を用いて映像中に埋め込むと同時に、第２の許可情報を第２の埋め込み方法を用いて映像に埋め込む方法がある。ここで、第１の埋め込み方法は削除が難しい方法、すなわち禁止情報の埋め込み方法に用いたのと同様の方法で埋め込みを行い、第２の埋め込み方法は画面の端に可視的に埋め込むなどの削除が容易な方法で埋め込みを行う。映像のコピーに際しては、第１の許可情報と第２の許可情報の両方がそろって検出されたときに始めてコピー可とし、第２の許可情報のみを削除する。このように第１の許可情報と第２の許可情報の組み合わせにより、検出と削除が容易であるが、その埋め込みが困難であるような埋め込み方法を実現することが可能となる。ここで示した第１の埋め込み方法は、禁止情報の埋め込み方法と全く同じ方法でも良いし、異なる方法でも良い。

【００７７】第１と第２の２つの許可情報を構成する方法としては、コードMを変換係数により変換処理した結果と、変換係数のいずれか一方を第１の許可情報とし、もう一方を第２の許可情報とする方法がある。ここで、変換処理とは、変換係数との加減乗除などの算術計算や、変換係数との論理演算や、変換係数を鍵とした暗号化処理や、変換係数を遅延量とした遅延処理など、変換係数の値によってその処理結果が変わるような処理であれば任意の方法を取ることが可能である。特に、コードMと変換結果から変換係数を求めることが困難であるような変換処理が望ましく、不正に対して強いという効果がある。これは、変換処理の方法を秘密にすることにより実現できる。

【００７８】（実施の形態２）本発明の実施の形態２として、実施の形態１で説明したデータ制御方法を実現するためのデータ制御システム、及び該システムにおけるデータ制御情報埋込装置とデータ制御情報情報検出装置を示す。

【００７９】図６は、本実施の形態２におけるデータ制御システムの構成図である。このデータ制御システムは、データ制御情報埋込装置４１、データ制御情報検出装置４２、伝送部４３、記録部４４、記録媒体４５を含んで構成される。

【００８０】データ制御情報埋込装置４１では、映像信号を入力してコピー制御情報を埋め込み、この情報が埋め込まれた映像信号を伝送部４３に出力する。

【００８１】伝送部４３による伝送方法として、衛星や地上波などを利用した無線によるデジタル伝送又はアナログ伝送が有る。又、電話線や同軸ケーブル、ツイストペアケーブル、光ケーブルなどを利用した有線によるデジタル伝送又はアナログ伝送がある。更には、磁気ディスク、光ディスク、ＣＤ、ＤＶＤ、ＤＶＣ、ＶＣＲなどのデジタル又はアナログの記録メディアも、該記録メディアから映像信号がビットストリームとして再生されるので伝送部４３と考える。

【００８２】伝送部４３を介して伝送もしくは再生された映像信号は、データ制御情報検出装置４２に入力される。データ制御情報検出装置４２では、コピー制御情報を検出し、コピー許可かコピー禁止かを示す記録可否フラグと映像情報を出力し、これらの情報が記録部４４に入力される。

【００８３】記録部４４は、記録可否フラグがコピー許可を示す場合は、記録媒体４５に映像情報の記録を許可し、コピー禁止を示す場合には記録を行わない。ここで記録媒体４５は、磁気ディスク、光ディスク、ＣＤ、ＤＶＤ、ＤＶＣ、ＶＣＲなどのデジタル又はアナログの記録メディアなど、データの記録を行う媒体であれば任意の媒体で良い。

【００８４】データ制御情報埋込装置４１は、禁止情報埋込手段４１１と許可情報埋込手段４１２を有している。

【００８５】データ制御情報埋込装置４１において、禁止情報埋込手段４１１は、一回コピー可又はコピー禁止の情報を埋め込みたい場合に、入力した映像信号に禁止情報を埋め込む。この埋め込み処理は、図２のステップＳ２の処理と同じである。次に、許可情報埋込手段４１２は、１回コピー可の場合に、許可情報を映像信号中に埋め込む。この許可情報埋込手段４１２の動作については後述する。この様なデータ制御情報埋込装置４１の動作により、コピーフリーの場合は映像に何も埋め込まれず、一回コピー可の場合には映像に禁止情報と許可情報とが埋め込まれ、コピー不可の場合には映像に禁止情報が埋め込まれる。

【００８６】データ制御情報検出装置４２は、禁止情報検出手段４２１、許可情報検出・削除手段４２２、判定手段４２３を有している。

【００８７】データ制御情報検出装置４２において、許可情報検出・削除手段４２２は映像信号から許可情報の検出及び削除を行う。許可情報が検出された場合には１を、検出されない場合には０を示す許可フラグが出力される。許可情報検出・削除手段４２２の動作については後述する。

【００８８】禁止情報検出手段４２１は、許可情報検出・削除手段４２２から映像信号を入力すると、埋め込まれた禁止情報の有無を調べる。ここで禁止情報が検出された場合には１を、検出されない場合には０を示す禁止フラグが出力される。許可フラグと禁止フラグの値は判定手段４２３に入力される。判定手段４２３は許可フラグが１の場合、又は禁止フラグが０の場合には、コピー許可を示す記録可否フラグを出力する。また許可フラグが０でかつ禁止フラグが１の場合には、コピー禁止を示す記録可否フラグを出力する。

【００８９】以上のデータ制御情報検出装置４２の動作により、許可情報が埋め込まれた映像は許可情報が削除された後でコピーが許可される。また、許可情報も禁止情報も埋め込まれていない映像は、コピーが許可される。更に許可情報が埋め込まれておらず、禁止情報が埋め込まれている映像は、コピーが禁止される。

【００９０】次に、許可情報埋込手段４１２及び許可情報検出・削除手段４2-2の構成と動作について図７及び図８を用いて説明する。

【００９１】図７に示すように許可情報埋込手段４１２は、署名埋込手段５１、コード抽出手段５２、署名手段５３を含んで構成される。

【００９２】許可情報埋込手段４１２においては、先ずコード抽出手段５２が、映像信号から一意に導き出せるコードMを生成して署名手段５３に出力する。署名手段５３はコードMをデジタル署名ｆ（M）に変換し、署名埋込手段５１に出力する。次に署名埋込手段５１は、映像信号中にデジタル署名ｆ（M）を埋め込む。許可情報を埋め込まない場合には、デジタル署名ｆ（M）の埋め込み処理は行わない。ここで、コード抽出手段５２におけるコードMの生成方法、署名手段５３における署名ｆ（M）の生成方法、署名埋込手段５１における署名の埋め込み方法は、図３のステップＳ２１、Ｓ２２、Ｓ２３の処理と夫々同様である。

【００９３】図８に示すように許可情報検出・削除手段４２２は、署名抜出・削除手段５４、コード抽出手段５５、認証手段５６を含んで構成される。

【００９４】許可情報検出・削除手段４２２においては、署名抜出・削除手段５４がデジタル署名ｆ（M）を映像信号から抜き出し、映像信号からデジタル署名ｆ（M）の少なくとも一部を削除する。次に、コード抽出手段５５は、コード抽出手段５２と同様に映像信号からコードMを生成して認証手段５６に出力する。次に、認証手段５６は、コードMを基にデジタル署名ｆ（M）を認証し、記録許可を示す記録可否フラグを出力する。また認証されなければ、記録禁止を示す記録可否フラグを出力する。ここで、署名抜出・削除手段５４における署名の抜き出し方法、コード抽出手段に５５におけるコードMの生成方法、認証手段５６における認証方法は図５で説明したものと夫々同様である。

【００９５】以上のように本実施の形態２によれば、コピーの禁止と許可だけでなく、１回だけコピーを許可するような制御を実現でき、従来の方法に比べて、不正がより困難であるデータ制御システム、及び該システムにおけるデータ制御情報埋込装置とデータ制御情報検出装置を実現できる。

【００９６】なお、本実施の形態２では、１回コピー可を実現する方法について述べたが、コピー制御情報を埋め込む時に許可情報をＮ（Ｎは１以上の自然数）回埋め込み、検出するときには許可情報が何個検出されても、１個だけ削除することにより、Ｎ回コピー可を実現することができる。

【００９７】また、コピー禁止情報の埋め込みと検出の方法について述べたが、再生禁止情報の埋め込みと検出の方法も同様に実現でき、再生の制御も行える。さらに、コピーの制御と再生の制御も同時に実現可能である。

【００９８】コピー制御情報埋込み装置４１については図６に示すような構成としたが、これに限られるものではない。禁止情報埋込手段４１１と許可情報埋込手段４１２の順序が逆でも良く、コピー不可の映像には少なくとも禁止情報を埋め込み、1回コピー可の映像には禁止情報と許可情報の両方を埋め込むような任意の構成の装置により実現可能である。

【００９９】コピー制御情報検出装置４２のについては、図６に示すような構成としたが、これに限られるものではない。許可情報検出削除手段４２２の前段の映像信号が禁止情報検出手段４２１に入力されるような構成でも良いし、許可情報検出削除手段４２２が許可情報検出手段と許可情報削除手段に分離されているような構成でも良く、許可情報が検出されるとコピーを許可して許可情報を削除し、禁止情報が検出されるとコピーを禁止するような任意の構成の装置により実現可能である。

【０１００】以上の説明では、許可信号として映像から一意に得られるコードMを元にしたデジタル署名を用いているが、これに限られるわけではなく、任意の埋め込み方法を用いることができる。即ち、ユーザＢに埋め込み方法を公開せず、削除と検出の方法のみを公開すれば良い。削除や検出の方法から、埋め込みの方法が類推できない方法や、削除や検出と比べて埋め込み処理の計算量が多いか、又は回路規模が複雑であるような方法であれば、更に不正に対して強くすることができる。この時、映像から一意に得られるコードMを元にして許可情報を作成することにより、映像と許可情報を１対１に対

応させることができ、許可情報の不正な作成を困難にする。

【０１０１】許可情報の埋め込み方法の他の例としては、許可情報が第１の許可情報と第２の許可情報の２つから構成され、第１の許可情報を第１の埋め込み方法を用いて映像中に埋め込むと同時に、第２の許可情報を第２の埋め込み方法を用いて映像に埋め込む方法がある。ここで、第１の埋め込み方法は削除が難しい方法、すなわち禁止情報の埋め込み方法に用いたのと同様の方法で埋め込みを行い、第２の埋め込み方法は画面の端に可視的に埋め込むなどの削除が容易な方法で埋め込みを行う。映像のコピーに際しては、第１の許可情報と第２の許可情報の両方がそろって検出されたときに始めてコピー可とし、第２の許可情報のみを削除する。このように第１の許可情報と第２の許可情報の組み合わせにより、検出と削除が容易であるが、その埋め込みが困難であるような埋め込み方法を実現することが可能である。ここで示した第１の埋め込み方法は、禁止情報の埋め込み方法と全く同じ方法でも良いし、異なる方法でも良い。

【０１０２】第１と第２の２つの許可情報を構成する方法としては、コードMを変換係数により変換処理した結果と、変換係数のいずれか一方を第１の許可情報とし、もう一方を第２の許可情報とする方法がある。ここで、変換処理とは、変換係数との加減乗除などの算術計算や、変換係数との論理演算や、変換係数を鍵とした暗号化処理や、変換係数を遅延量とした遅延処理など、変換係数の値によってその処理結果が変わるような処理であれば任意の方法を取ることが可能である。特に、コードMと変換結果から変換係数を導くことが困難であるような変換処理が望ましく、不正に強いという効果が得られる。これは、変換処理の方法を秘密にすることにより実現できる。

【０１０３】なお、上記各実施形態１及び２においては、データ制御情報埋め込み方法あるいはデータ制御情報埋め込み装置は、ステータスがコピーフリーの時に禁止情報も許可情報も埋め込まないとしたが、これに限られるものではない。ステータスがコピーフリーを示すときには、コピーフリーを示す情報を埋め込んでも良く、同様の効果が得られる。

【０１０４】また、データ制御情報検出方法あるいはデータ制御情報検出装置においては、コピー制御情報が検出されないときには、コピーを許可するとしたが、これに限られるものではない。何も情報が検出されないときには、コピー禁止としても良い。また、コピーフリーを示す情報が検出されたときにはコピー可とするような構成としても良く、同様の効果が得られる。

【０１０５】

【発明の効果】以上の様に、本発明によれば、コピーフリーとコピー禁止だけでなく、データに許可情報が検出されたとき、Ｎ回のコピーのみを許すことができる。そして不正行為が困難なデータ制御方法を実現できる。

【０１０６】１実施形態によれば、データの作り手側で、許可情報をデジタル署名を用いて挿入しているため、データを入手した側での許可情報の改ざんは不可能となる。

【０１０７】１実施形態によれば、コピーフリーとコピー禁止の制御だけではなく、Ｎ回のコピーを許可する情報も埋め込むことができる。

【０１０８】また、１実施形態によれば、データから一意に得られるコードを元に許可情報を生成しているため、許可情報はデータと１対１に対応し、許可情報の改ざんを困難にすることが出来る。

【０１０９】１実施形態によれば、許可情報がデジタル署名を用いて挿入されているため、データを入手した側での許可情報の改造は不可能となる。

【０１１０】１実施形態によれば、許可情報の挿入されたデータが入力されたとき、コピー回数をＮ回に制限し、禁止情報のみが挿入されたデータが入力されたとき、コピーを禁止することができる。

【０１１１】１実施形態によれば、データから一意に得られるコードを元にした許可情報が検出されたときにのみ、コピーを許可する。

【０１１２】１実施形態によれば、デジタル署名が認証されたときにのみ、コピーが許可される。

【０１１３】１実施形態によれば、データより許可情報が検出されたとき、そのデータを記録媒体に記録することができる。

【０１１４】１実施形態によれば、データに禁止情報のみが検出されたとき、データ処理を禁止し、許可情報が検出されたとき、Ｎ回のデータ処理を許すことができる。

【０１１５】１実施形態によれば、データ処理の禁止の制御だけではなく、Ｎ回のデータ処理を許可する情報も埋め込むことができる。

【０１１６】１実施形態によれば、許可情報の挿入されたデータが入力されたとき、データ処理回数をＮ回に制限し、禁止情報のみが挿入されたデータが入力されたとき、データ処理を禁止することができる。

【０１１７】１実施形態によれば、許可情報の挿入されたデータが入力されたとき、データ処理回数をＮ回に制限し、禁止情報のみが挿入されたデータが入力されたとき、データ処理を禁止することができる。

【図面の簡単な説明】

【図１】実施の形態１のデータ制御方法の概要を示す説明図である。

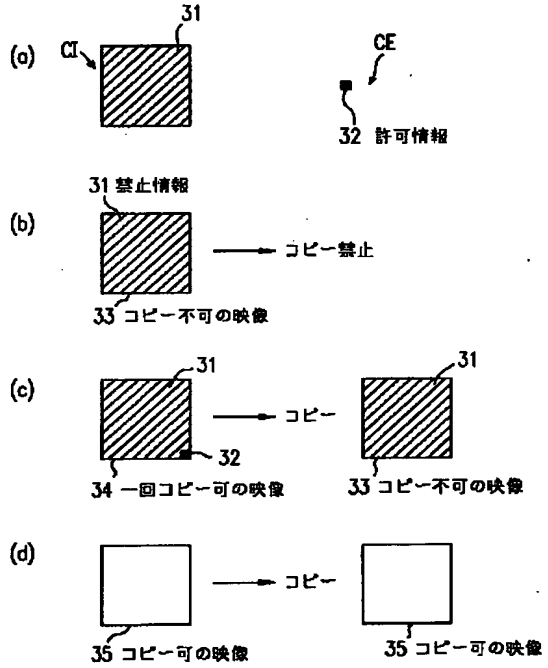
【図２】実施の形態１のデータ制御情報埋込方法を示すフローチャートである。

【図３】図２のデータ制御情報埋込方法の１処理を示すフローチャートである。

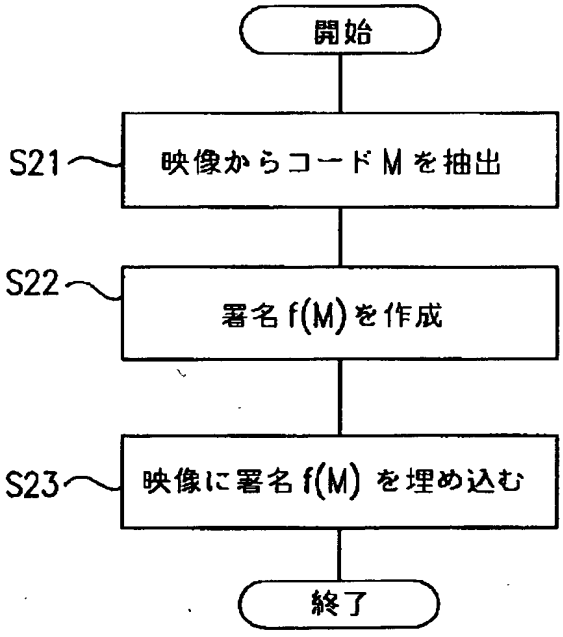
【図４】実施の形態１のデータ制御情報検出方法を示す

フローチャートである。
【図５】図４のデータ制御情報検出方法の１処理を示すフローチャートである。
【図６】本実施の形態２におけるデータ制御システムの構成図である。
【図７】図６のデータ制御システムにおける許可情報埋込手段の構成図である。
【図８】図６のデータ制御システムにおける許可情報検出手段の構成図である。
【符号の説明】
４１　データ制御情報埋込装置
４２　データ制御情報検出装置
４３　伝送部
＊４４　記録部
４５　記録媒体
５１　署名埋込手段
５２，５５　コード抽出手段
５３　署名手段
５４　署名抜出・削除手段
５６　認証手段
４１１　禁止情報埋込手段
４１２　許可情報埋込手段
４２１　禁止情報検出手段
４２２　許可情報検出・削除手段
４２３　判定手段

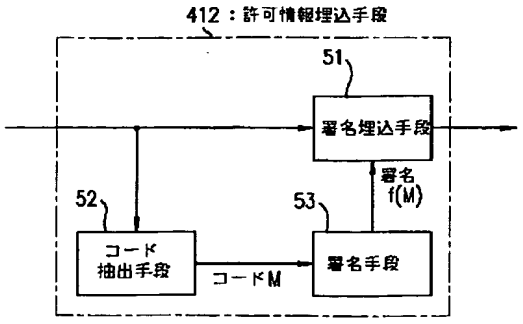
【図１】



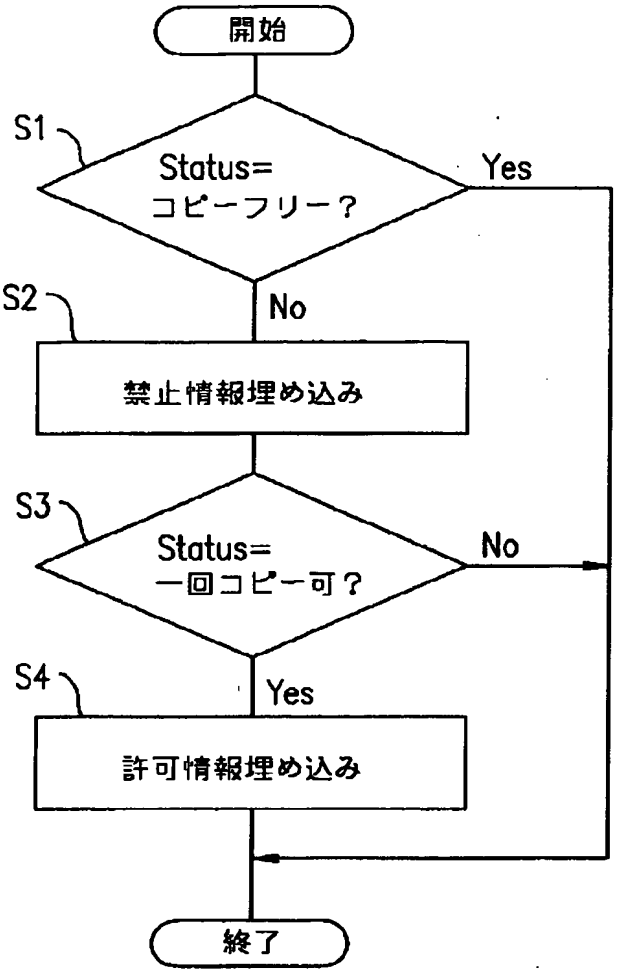
【図３】



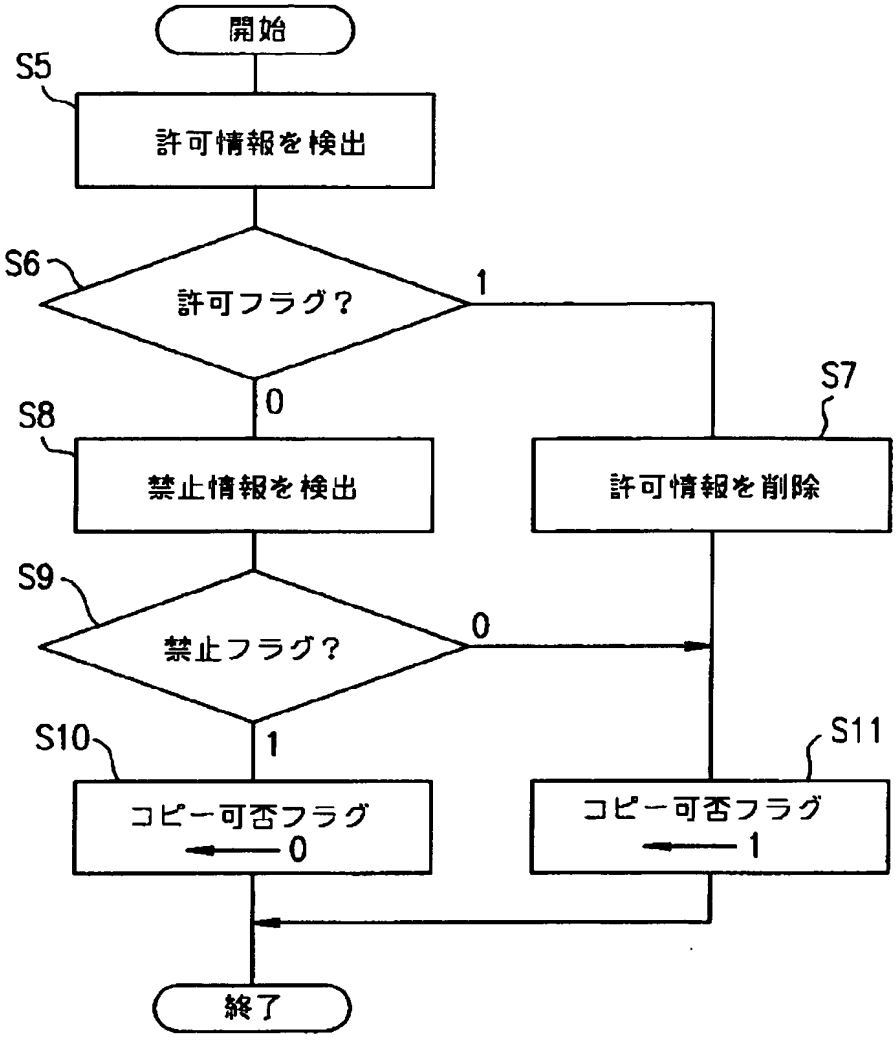
【図７】



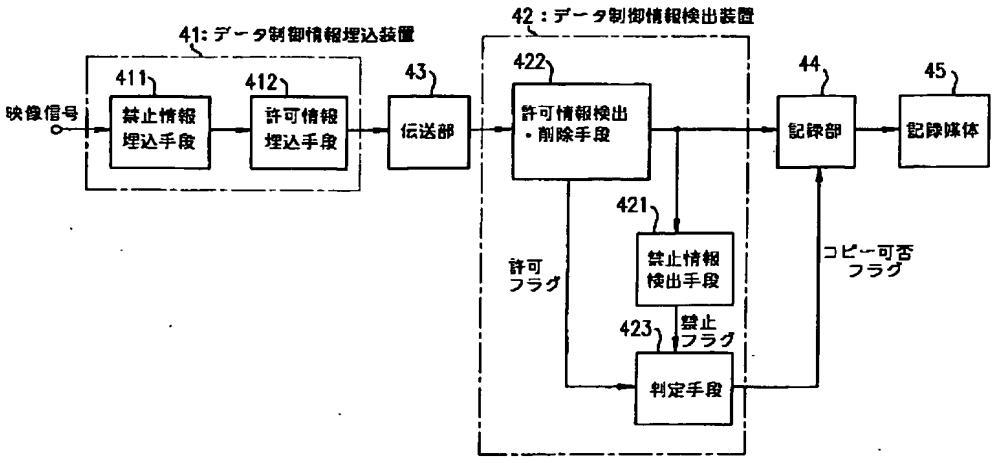
【図２】


開始
S1
Status=
コピーフリー？
Yes
No
S2
禁止情報埋め込み
S3
Status=
一回コピー可？
No
Yes
S4
許可情報埋め込み
終了

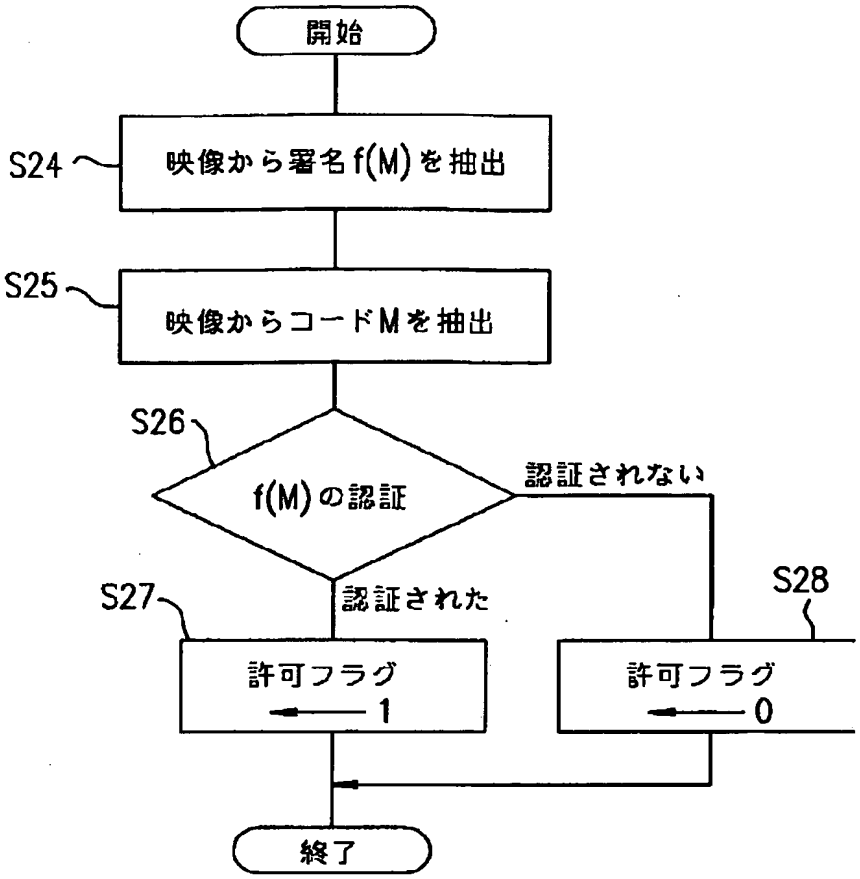
【図４】


開始
S5
許可情報を検出
S6
許可フラグ？
1
0
S7
S8
禁止情報を検出
許可情報を削除
S9
禁止フラグ？
0
1
S10
S11
コピー可否フラグ
←0
コピー可否フラグ
←1
終了

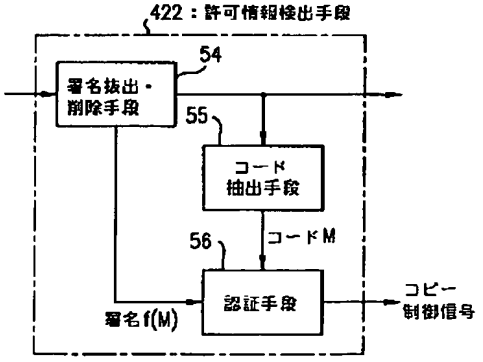
【図６】


41：データ制御情報埋込装置
42：データ制御情報検出装置
映像信号
411
禁止情報
埋込手段
412
許可情報
埋込手段
43
伝送部
422
許可情報検出
・削除手段
44
記録部
45
記録媒体
421
禁止情報
検出手段
許可
フラグ
コピー可否
フラグ
423
禁止
フラグ
判定手段

【図５】



【図８】



フロントページの続き

(51)Int.Cl.[6]		識別記号	FI		
H04N	1/387		H04L	9/00	675B
	5/91		H04N	5/91	P

7/08
7/081

7/08 Z